

Wprowadzenie do Cyberbezpieczeństwa

Anna Czacharowska

CSR Program Manager

aczachar@cisco.com



Cisco jest liderem globalnych zmian w zakresie zapewnienia cyfrowego bezpieczeństwa w obliczu cyfryzacji.



Innowacyjne
Rozwiązania
Technologiczne



Zaufany Lider



Partnerstwa
globalne



Lider
Technologii w
Obszarze
Cybersecurity



Spółeczna
Odpowiedzialność
Biznesu



 Networking
Academy

Dlaczego Cisco
Networking
Academy?

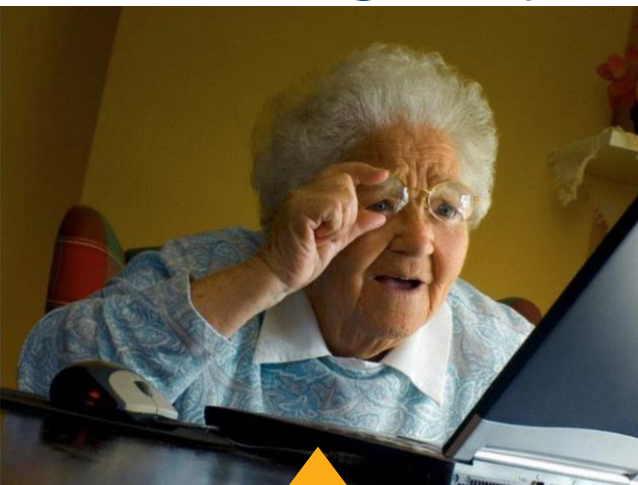


Partnerstwo w programie Cisco Networking Academy pozwala zapewnić słuchaczom wysoką jakość kształcenia i stale aktualizowane materiały edukacyjne.



Dzięki kształceniu kadr w oparciu o wysokiej jakości materiały dydaktyczne programu Cisco Netacad, instytucje budują świadomość zagrożeń wśród swoich pracowników i mogą aktywnie bronić się przed cyberprzestępstwami oraz zwiększać odporność na cyberataki , jednocześnie kreując bardziej produktywne i odpowiedzialne środowisko pracy.

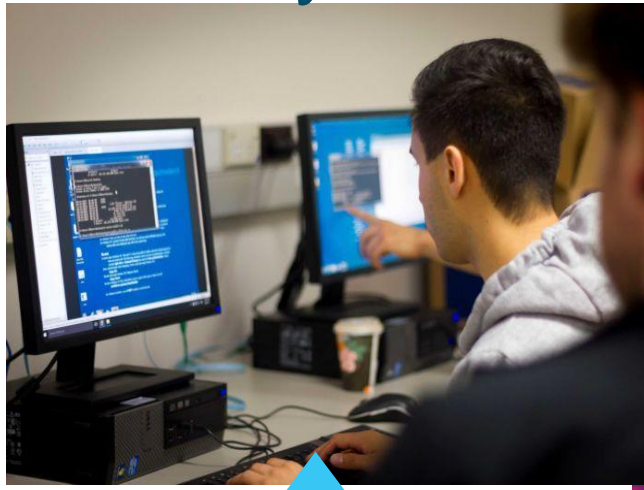
Dlaczego Cybersecurity?



Cyberhigiena

Każdy użytkownik internetu powinien znać podstawy i zastosowania cyberbezpieczeństwa, ponieważ to, co dzieje się w internecie może dotyczyć również nas wszystkich

Source: [Why Cybersecurity Starts at Home](#)



Deficyt umiejętności

Raport Frost & Sullivan oraz (ISC)² wskazują, że do roku 2020 na globalnym rynku pracy będzie brakowało ponad 1.5 miliona pracowników w obszarze cybersecurity

Source: [report](#)




Rynek pracy

Na 10 najważniejszych umiejętności wskazywanych przez pracodawców cyberbezpieczeństwo jest na miejscu TRZECIM.

Source: [CIO from IDG](#) , [Indeed.com](#)






























The Networking Academy - oferta kursów

 Przygotowuje do certyfikacji

 Wymagane szkolenie instruktorskie

 Do samodzielnej nauki



	Exploratory	Foundational	Career-Ready
Networking		 Networking Essentials  Mobility Fundamentals	  CCNA R&S: Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks   CCNP R&S: Switch, Route, TShoot Emerging Tech Workshop: Network Programmability Using Cisco APIC-EM*
Security	 Introduction to Cybersecurity	 Cybersecurity Essentials	  CCNA Security   CCNA Cyber Ops*
IoT & Analytics	 Introduction to IoT	 IoT Fundamentals: Connecting Things, Big Data & Analytics Hackathon Playbook, IoT Security*	
OS & IT	 NDG Linux Unhatched	  NDG Linux Essentials   IT Essentials	 NDG Linux I  NDG Linux II
Programming		 CLA: Programming Essentials in C  CPA: Programming Essentials in C++  PCA: Programming Essentials in Python* Emerging Tech Workshop: Experimenting with REST APIs Using Cisco Spark*	 CLP: Advanced Programming in C*  CPP: Advanced Programming in C++
Business	 Be Your Own Boss	 Entrepreneurship	
Digital Literacy	 Get Connected		

Wprowadzenie do Cyberbezpieczeństwa

Opis kursu

Przedstawia trendy, typowe zagrożenia i sposoby zabezpieczeń cyber danych prywatnych i firmowych

Korzyści

Dowiesz się, jak chronić swoje dane, jak zachować prywatność online oraz dlaczego świadomość zagrożeń i znajomość sposobów zabezpieczenia jest kluczowa dla wszystkich obszarów IT.

Elementy kursu

- 5 modułów
- Interaktywne treści
- 8 ćwiczeń i 7 laboratoriów dla praktycznego utrwalenia wiadomości
- 4 testy and 1 test końcowy
- Linki do zasobów dodatkowych



Cechy

Dla kogo: uczniowie, studenci, pracownicy

Wymagania wstępne: Nie ma

Szkolenie Instruktorskie: Nie jest wymagane

Model kształcenia: kurs prowadzony przez instruktora lub do nauki samodzielnej (Self-paced)

Czas realizacji: 15 godzin

Rozdziały i treści kursu

Rozdział	TYTUŁ	OPIS
1	Zapotrzebowanie na cyberbezpieczeństwo	<ul style="list-style-type: none">• Dlaczego cyberbezpieczeństwo jest takie istotne.• Charakterystyka i wartość danych prywatnych i danych w organizacjach (firmach, instytucjach)
2	Ataki, Konceptcje i Techniki	<ul style="list-style-type: none">• Charakterystyka i przebieg cyberataku• Trendy w cyberzagrożeniach
3	Ochrona prywatności i danych	<ul style="list-style-type: none">• Jak chronić swoje urządzenia.• Jak zachować bezpieczeństwo i prywatność w cyberprzestrzeni
4	Ochrona Organizacji	<ul style="list-style-type: none">• Techniki zabezpieczenia organizacji przed cyberatakami
5	Czy wiążesz swoją przyszłość z cyberbezpieczeństwem?	<ul style="list-style-type: none">• Rozumienie prawnych i etycznych wyzwań w zakresie cyberbezpieczeństwa• Kierunki rozwoju ścieżki edukacyjnej i kariery w zakresie cyberbezpieczeństwa

Moduł 1: Zapotrzebowanie na Cyberbezpieczeństwo?



Dowiedz się czym w ogóle jest cyberbezpieczeństwo i dlaczego tak szybko rośnie zapotrzebowanie na specjalistów w tym zakresie

Moduł 1:

- Czym jest tożsamość online, jak jest wartość danych i dlaczego są one interesujące dla cyberprzestępców.
- Czym są dane organizacji i dlaczego należy je chronić.
- Czym jest wojna cybernetyczna i dlaczego organizacje, instytucje i rządy potrzebują specjalistów ds. bezpieczeństwa cybernetycznego, aby chronić swoich obywateli i infrastrukturę



Moduł 2: Ataki, Koncepcje i Techniki



Dowiesz się jak specjaliści cyberbezpieczeństwa analizują cyberatak.

Moduł 2:

- Luki w zabezpieczeniach, różne typy podatności i różne rodzaje złośliwego oprogramowania
- Techniki wykorzystywane przez przestępców do infiltracji systemów
- Charakterystyka i przebieg cyberataku.
- Trendy w zagrożeniach cybernetycznych



Moduł 3: Zabezpieczenie danych i prywatności



Bądź świadomy i dowiedz się, jak zabezpieczyć swoje urządzenia i dane.

Moduł 3 :

- Wskazówki dotyczące ochrony urządzeń osobistych i danych online
- Metody uwierzytelniania, bezpieczne przechowywanie danych, proste wskazówki jak zachować bezpieczeństwo w internecie
- Ochrona urządzeń przed zagrożeniami.
- Ochrona prywatności.



Moduł 4: Ochrona Organizacji



Naucz się, jakie techniki, procesy są stosowane dla ochrony sieci w organizacjach i jakie są najlepsze praktyki w tym zakresie.

Moduł 4 :

- Sprzęt, dane i powszechnie stosowane techniki takie jak botnety czy kill chain.
- Podejście Cisco do cyberbezpieczeństwa z wykorzystaniem zespołu CSIRT oraz security playbook.
- Techniki zabezpieczeń instytucji przed atakami cybernetycznymi.
- Co to jest behavior-based approach to cybersecurity.



Moduł :5 Czy wiążesz swoją przyszłość z cyberbezpieczeństwem?



Poznaj ścieżki certyfikacyjne i specjalizacje w zakresie cyberbezpieczeństwa oraz etyczne i prawne aspekty w tym obszarze
Moduł 5:

- Prawne i etyczne aspekty w obszarze cyberbezpieczeństwa
- Poznaj możliwości dalszej edukacji i rozwoju zawodowego w obszarze cyberbezpieczeństwa



Informacje dodatkowe

Odwiedź stronę [Course information page](#) na Cisco NetAcad.com, aby uzyskać dodatkowe informacje.



Model prowadzenia zajęć

Zarejestruj słuchaczy w swojej Akademii Cisco poprzez -
uruchomienie klasy i **zajęcia z instruktorem w trybie
online lub stacjonarnym**
- **w trybie e-learning do samodzielnej nauki** (i samodzielnej
rejestracji) po wygenerowaniu linku przez instruktora danej
akademii

Nie jest wymagane szkolenie instruktorskie od osoby
prowadzącej zajęcia



Kontynuacja nauki

Zasoby dodatkowe dla Instruktor

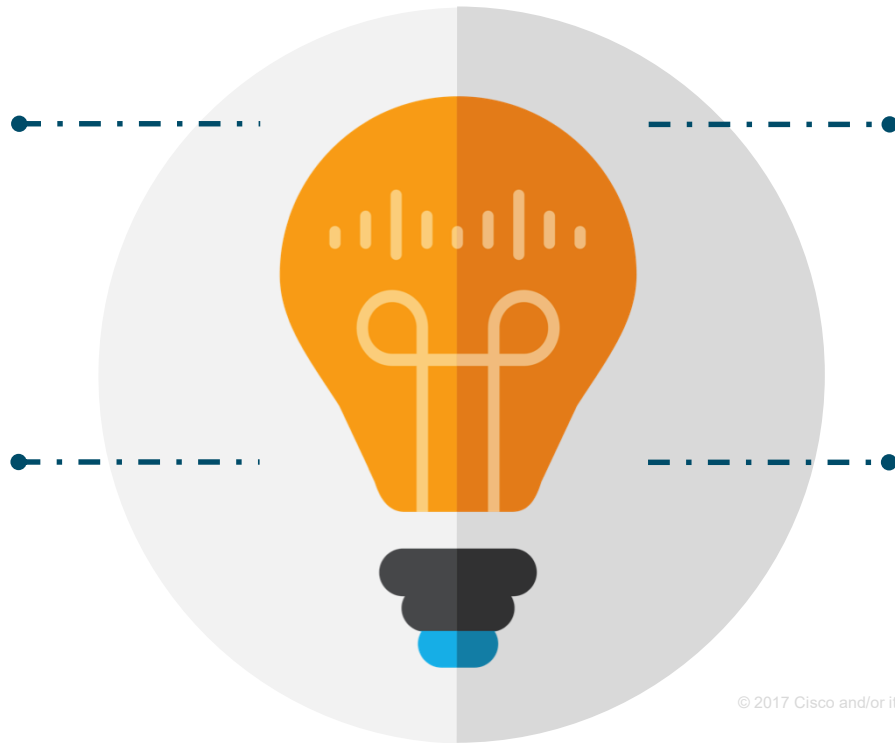
<https://www.netacad.com/group/resources/cybersecurity/2.1>

PPT

Prezentacje dla
Instruktora
Intro to Cybersecurity
Video

FAQ

Najczęściej zadawane
pytania



S&S

Scope & Sequence
Dokument

Plus

Materiały uzupełniające

Cybersecurity Essentials (w jęz. ang)

Opis

Kurs buduje wiedzę i podstawowe umiejętności w zakresie wszystkich dziedzin cyberbezpieczeństwa, w tym bezpieczeństwa informacji, bezpieczeństwa systemów, bezpieczeństwa sieci, wraz z aspektami etyki i prawa oraz technikami obrony i łagodzenia skutków ataków stosowanych w ochronie organizacji.

Korzyści

Kurs rekomendowany dla osób pracujących z sieciami lub kształcących się w ramach CCNA. Kształci umiejętności w zakresie podstaw bezpieczeństwa dla osób pracujących w różnych rolach w IT

Elementy kursu

- 8 rozdziałów
- 34 ćwiczenia interaktywne, 10 ćwiczeń na symulator Cisco Packet Tracer, 12 praktycznych labów
- 8 testów, 1 egzamin końcowy
- Linki do materiałów uzupełniających



Cechy

Dla kogo? uczniowie, studenci i pracownicy

Wymagania wstępne: Introduction to Cybersecurity

Szkolenie Instruktorskie: nie jest wymagane

Model nauki: zajęcia z instruktorem lub e-learning

Czas realizacji: 30 godz

Rekomendowany kolejny kurs: CCNA R&S (wprowadzenie do sieci) oraz / lub CCNA Cybersecurity Operations

CCNA Cybersecurity Operations (w jęz. ang)

Opis

Przedstawia podstawowe koncepcje bezpieczeństwa i kształci umiejętności niezbędne do monitorowania, wykrywania, analizowania i reagowania na cyberprzestępczość, cyberszpiegostwo, zagrożenia, wymogi regulacyjne i inne problemy związane z bezpieczeństwem cybernetycznym, przed którymi stają organizacje. Podkreśla praktyczne zastosowanie umiejętności niezbędnych do utrzymania i zapewnienia gotowości operacyjnej bezpiecznych systemów sieciowych.

Korzyści

Umiejętności zdobyte w ramach kursu przygotowują do kariery w szybko rozwijającym się obszarze bezpieczeństwa cybernetycznego, ze szczególnym uwzględnieniem pracowników w centrach bezpieczeństwa (Security Operations Centers)

Elementy kursu

- 13 rozdziałów
- Laboratoria, ćwiczenia praktyczne z użyciem maszyn wirtualnych
- Ćwiczenia na Cisco® Packet Tracer (PT 7.0)
- Testy praktyczne, certyfikacyjne quizy i egzamin końcowy



PRZYGOTOWANIE
DO CERTYFIKACJI

Cechy

Dla kogo: Słuchacze kierunków informatycznych i pokrewnych lub profesjonalści (pracownicy IT) zainteresowani obszarem cyberbezpieczeństwa

Wymagania wstępne: Nie ma (rekomendowana znajomość linuxa i podstawowa znajomość sieci)

Współpraca z Academy Support center: Wymagana

Szkolenie Instruktorskie: Wymagane

Model kształcenia: Zajęcia z instruktorem

Czas realizacji: 70 godzin

